Installation of Zeek on Ubuntu 20

Version 20220518

- Deploy a VM from "Templ_Ubuntu_Server_20.04"
- Make sure the network is connected to something
- Make sure your deployed VM received an IP-address from DHCP or otherwise set a manual IP-address (see instruction in the login banner) and has Internet access
- Now perform the following:
  ```
  sudo apt update
  sudo apt upgrade
  ```
- In next step, we enable package installation from an external source (connect to your VM with SSH to copy-and-paste) by copying the following oneliners (*make sure they stay oneliners when copying and pasting!*):

  ```
  echo 'deb
  http://download.opensuse.org/repositories/security:/zeek/xUbuntu_20.04/ /'
  | sudo tee /etc/apt/sources.list.d/security:zeek.list

  curl -fsSL
  https://download.opensuse.org/repositories/security:zeek/xUbuntu_20.04/Rel
  ease.key | gpg --dearmor | sudo tee
  /etc/apt/trusted.gpg.d/security_zeek.gpg > /dev/null

  curl -fsSL
  https://download.opensuse.org/repositories/security:zeek/xUbuntu_20.04/Rel
  ease.key | gpg --dearmor | sudo tee
  /etc/apt/trusted.gpg.d/security_zeek.gpg > /dev/null

  sudo apt update
  sudo apt install zeek-lts
  ```

- *When asked for Postfix mail configuration, choose "no configuration"*
- Now execute
  ```
  export PATH=/opt/zeek/bin:$PATH
  ```
- Now follow the quick start guide steps 1-2-3 https://docs.zeek.org/en/current/quickstart/index.html and edit the following config files according your own network (private VLAN):
  - **`sudo nano /opt/zeek/etc/node.cfg`**

    interface=ens160
  - **`sudo nano /opt/zeek/etc/networks.cfg`**

    only your local LAN or DMZ
  - **`sudo nano /opt/zeek/etc/zeekctl.cfg`**

    LogRotationInterval = 86400

    MailConnectionSummary = 0

    MailHostUpDown = 0
- Continue the quick start guide and start the control application:
  - **`sudo /opt/zeek/bin/zeekctl`**
  - **`check`**
  - **`deploy`**
  - **`status`**
  - **`exit`**
- *Note: If there are errors after **`deploy`**, you can view the details with the diag command. If started successfully, the Zeek instance will begin analyzing traffic according to a default policy and output the results in directory /opt/zeek/logs/current and it keeps running after exiting the control application*
- If zeek started properly you can access the log files from the command line:
  - **`sudo chmod 777 -R /opt/zeek/logs`**
  - **`sudo chmod 777 -R /opt/zeek/spool`**
  - **`cd /opt/zeek/logs/current`**

- Now browse the log files and analyse some of them. Live logging can be viewed with the tail -f command (stop with CTRL-C). You should see al machines traffic being analysed in separate log files and all connections should appear anyway in the conn.log (= Flow Logging):
    - `tail -f /opt/zeek/logs/current/conn.log`
- Check al logfiles and explain what you see. Determine if the entries in weird.log and notice.log can be regarded as false-postives. Show relevant log lines (or screenshots) in your portfolio. *Note: Check the "Browsing Log Files" section of the mentioned quick start guide for more explanation about the (other) log files.*

Resources:
Instruction: https://kifarunix.com/install-zeek-on-ubuntu/
Software repository: https://software.opensuse.org/download.html?project=security%3Azeek&package=zeek-lts#manualUbuntu
Installation of Zeek: https://docs.zeek.org/en/current/install/install.html
Quick Start Guide for Zeek: https://docs.zeek.org/en/current/quickstart.html